ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 126 (2007) 68–73

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Bounds of incomplete multiple Kloosterman sums

Igor E. Shparlinski

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

Received 12 September 2006

Available online 23 December 2006

Communicated by Wenzhi Luo

Abstract

We obtain an estimate for incomplete multiple Kloosterman sums modulo a prime which improves the previous result of W. Luo.

1. Introduction

Let p be a prime. Given an integer n with $\gcd(n, p) = 1$, we use $\bar{n}$ to denote the modular inverse of n, that is, $n\bar{n} \equiv 1 \pmod{p}$, $1 \leqslant n < p$. We also define $\mathbf{e}_p(z) = \exp(2\pi i z/p)$.

We consider incomplete s-dimensional Kloosterman sums

$$K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p) = \sum_{n_1=M_1+1}^{M_1+N_1} \cdots \sum_{n_s=M_s+1}^{M_s+N_s} \mathbf{e}_p(a_1 n_1 + \cdots + a_s n_s + a_{s+1}\overline{n_1 \cdots n_s}),$$

with integer vectors $\mathbf{a} = (a_1, \ldots, a_{s+1}) \in \mathbb{Z}^{s+1}$ and $\mathbf{N} = (N_1, \ldots, N_s)$, $\mathbf{M} = (M_1, \ldots, M_s) \in \mathbb{Z}^s$ such that $0 \leqslant M_\nu < M_\nu + N_\nu < p$, $\nu = 1, \ldots, s$. We obtain a new estimate on the sums which improves the previous estimate of W. Luo [12].

As in [12] we use the bounds of D.A. Burgess [3] on incomplete Gauss sums. However we also add a new ingredient and use bounds of such sums on average over all multiplicative characters, for example the recent bound of A. Ayyad, T. Cochrane and Z. Zheng [1, Theorem 2].

E-mail address: igor@ics.mq.edu.au.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.12.003

The bound of J. Bourgain [2] can also be used to obtain nontrivial estimates for Kloosterman sums modulo a prime p, for example for sums $K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p)$ with

$$N_1 \cdots N_s \geqslant p^{s/4+\varepsilon}$$

for $s \geqslant 2$ and any fixed $\varepsilon > 0$, provided that p is sufficiently large. However, in the cases when our bound applies, it is more explicit. Furthermore, the bound of [2] does not seem to extend to Kloosterman sums modulo an arbitrary integer q, while all ingredients of our approach are readily available for composite moduli q as well, see [4–6] (although technically they look slightly differently).

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' may depend on integer parameters r and s. We recall that the notations $U = O(V)$ and $V \ll U$ are both equivalent to the assertion that the inequality $|U| \leqslant cV$ holds for some constant $c > 0$.

Theorem 1. *For any integer $s \geqslant 2$, uniformly over all integer vectors $\mathbf{a} = (a_1, \ldots, a_{s+1}) \in \mathbb{Z}^{s+1}$, $\mathbf{N} = (N_1, \ldots, N_s)$, $\mathbf{M} = (M_1, \ldots, M_s) \in \mathbb{Z}^s$ such that $0 \leqslant M_\nu < M_\nu + N_\nu < p$, $\nu = 1, \ldots, s$, and $\gcd(a_{s+1}, p) = 1$, and any integer $r \geqslant 2$, we have*

$$K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p) \ll N_1 \cdots N_s p^{-1} + (N_1 \cdots N_s)^{1-(r+s-2)/rs} p^{1/2+(s-2)/4(r-1)} (\log p)^{2s-4}.$$

We note that the bound of W. Luo [12] asserts that under the conditions of Theorem 1 we have the bound

$$K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p) \ll N_1 \cdots N_s p^{-1} + (N_1 \cdots N_s)^{1-1/r} p^{1/2+s/4(r-1)} (\log p)^{2s}, \tag{1}$$

which is weaker than that of Theorem 1. In fact in [12] only the case $M_1 = \cdots = M_s = 0$, $a_1 = \cdots = a_{s+1} = 1$, has been considered, however the proof extends to the general case without any changes.

In the case of $s \geqslant 4$ we obtain a better bound.

Theorem 2. *For any integer $s \geqslant 4$, uniformly over all integer vectors $\mathbf{a} = (a_1, \ldots, a_{s+1}) \in \mathbb{Z}^{s+1}$, $\mathbf{N} = (N_1, \ldots, N_s)$, $\mathbf{M} = (M_1, \ldots, M_s) \in \mathbb{Z}^s$ such that $0 \leqslant M_\nu < M_\nu + N_\nu < p$, $\nu = 1, \ldots, s$, and $\gcd(a_{s+1}, p) = 1$ and any integer $r \geqslant 2$, we have*

$$K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p) \ll N_1 \cdots N_s p^{-1} + (N_1 \cdots N_s)^{1-(s-4)/rs} p^{-1/2+(s-4)/4(r-1)} W (\log p)^{2s-4},$$

where

$$W = \prod_{\nu=1}^{s} \bigl(1 + p^{1/s} N_\nu^{-2/s} (\log p)^{2/s}\bigr).$$

Clearly, if more information about the size of $N_1, \ldots, N_s$ is available then the bound of Theorem 2 can be simplified.

For example, for short sums where $N_\nu \leqslant p^{1/2} \log p$, $\nu = 1, \ldots, s$, Theorem 2 implies the estimate

$$K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p) \ll N_1 \cdots N_s p^{-1} + (N_1 \cdots N_s)^{1-(2r+s-4)/rs} p^{1/2+(s-4)/4(r-1)} (\log p)^{2s-2}.$$

Table 1

s	Bound (1), α_s, r	Theorem 1, β_s, r	Theorem 2, β_s, r
2	$\alpha_2 = 1, r = 2$	$\beta_2 = 1/2, r = 2$	–, –
3	$\alpha_3 = 5/6, r = 2$	$\beta_3 = 7/15, r = 4$	–, –
4	$\alpha_5 = 3/4, r = 3$	–, –	$\beta_4 = 1/4, r = 2$
5	$\alpha_5 = 27/40, r = 3$	–, –	$\beta_5 = 1/4, r \to \infty$

On the other hand, if $N_\nu \geqslant p^{1/2} \log p$, $\nu = 1, \ldots, s$, then we obtain

$$K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p) \ll N_1 \cdots N_s p^{-1} + (N_1 \cdots N_s)^{1-(s-4)/rs} p^{-1/2+(s-4)/4(r-1)} (\log p)^{2s-4}.$$

For arbitrary $N_1, \ldots, N_s$ the nontriviality ranges for the bound (1) and our results are not easy to describe in a concise way. Instead, here we present the values of α_s and β_s, such that if $N_1 = \cdots = N_s = N$ then for arbitrary $\varepsilon > 0$, the bound (1) and the implied by a combination of Theorems 1 and 2 are nontrivial whenever

$$N \geqslant p^{\alpha_s+\varepsilon} \quad \text{and} \quad N \geqslant p^{\beta_s+\varepsilon},$$

respectively. We also present the corresponding optimal choice of r (see Table 1).

In fact, it is easy to see that we can take $\beta_s = 1/4$ for every $s \geqslant 4$, while the bound (1), taken with either $r = \lfloor \sqrt{s/2} + 1 \rfloor$ or $r = \lceil \sqrt{s/2} + 1 \rceil$, implies that

$$\alpha_s = \frac{1}{4} + \frac{1}{\sqrt{2s}} + O\bigl(s^{-1}\bigr)$$

as $s \to \infty$.

2. Multiplicative character sums

Let $\mathcal{X}_p$ be the set of all $p-1$ multiplicative characters modulo p. We refer to [11] for definitions and basic properties of multiplicative characters. In particular, we recall that for $u \in Z$,

$$\frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} \chi(u) = \begin{cases} 1 & \text{if } u \equiv 1 \pmod p, \\ 0 & \text{otherwise,} \end{cases} \tag{2}$$

see [11, Theorem 5.4]. We also use χ_0 to denote the principal character.

We need bounds of *incomplete Gauss sums*

$$S_{a,\chi}(M, N; p) = \sum_{n=M+1}^{M+N} \chi(n) \mathbf{e}_p(an).$$

In particular we recall that for $M = 0$ and $N = p \geqslant 3$, that is, for complete sums $S_{a,\chi}(p) = S_{a,\chi}(0, p; p)$, we have

$$\bigl|S_{a,\chi}(p)\bigr| = \begin{cases} p^{1/2} & \text{if } \chi \neq \chi_0, \\ 1 & \text{if } \chi = \chi_0, \end{cases} \tag{3}$$

provided $\gcd(a, p) = 1$.

We now recall the following estimate of D.A. Burgess [3].

Lemma 3. *For any positive integers $0 \leqslant M < M + N < p$, a nonprincipal character $\chi \in \mathcal{X}_p$ and an arbitrary integer a, the bound*

$$\left|S_{a,\chi}(M, N; p)\right| \ll N^{1-1/r} p^{1/4(r-1)} (\log p)^2$$

holds with arbitrary positive integer r.

We also need some bounds "on average."

Lemma 4. *For any positive integers $0 \leqslant M < M + N < p$, and an arbitrary integer a, we have*

$$\sum_{\chi \in \mathcal{X}_p} \left|S_{a,\chi}(M, N; p)\right|^2 = N(p-1).$$

Proof. We recall that if $\gcd(n, p) = 1$, then for the conjugated character $\overline{\chi}$ we have $\overline{\chi}(n) = \chi(\overline{p})$. Therefore

$$\begin{aligned}\sum_{\chi \in \mathcal{X}_p} \left|S_{a,\chi}(M, N; p)\right|^2 &= \sum_{\chi \in \mathcal{X}_p} \sum_{m,n=M+1}^{M+N} \chi(m\overline{n})\mathbf{e}_p\big(a(m-n)\big) \\ &= \sum_{m,n=M+1}^{M+N} \mathbf{e}_p\big(a(m-n)\big) \sum_{\chi \in \mathcal{X}_p} \chi(m\overline{n}) = N(p-1)\end{aligned}$$

since the inner sum vanishes unless $n = m$ in which case it is equal to $p - 1$. □

The following estimate of the 4th moment of $S_{a,\chi}(M, N, p)$ follows a result of A. Ayyad, T. Cochrane and Z. Zheng [1].

Lemma 5. *For any positive integers $0 \leqslant M < M + N < p$, and an arbitrary integer a, we have*

$$\sum_{\chi \in \mathcal{X}_p} \left|S_{a,\chi}(M, N; p)\right|^4 \ll N^4 + N^2 p (\log p)^2.$$

Proof. As in the proof of Lemma 4 we obtain

$$\begin{aligned}\sum_{\chi \in \mathcal{X}_p} \left|S_{a,\chi}(M, N; p)\right|^4 &= \sum_{m_1,m_2,n_1,n_2=M+1}^{M+N} \mathbf{e}_p\big(a(m_1 + m_2 - n_1 - n_2)\big) \sum_{\chi \in \mathcal{X}_p} \chi(m_1 m_2 \overline{n_1}\,\overline{n_2}) \\ &\leqslant \sum_{m_1,m_2,n_1,n_2=M+1}^{M+N} \left| \sum_{\chi \in \mathcal{X}_p} \chi(m_1 m_2 \overline{n_1}\,\overline{n_2}) \right|.\end{aligned}$$

The inner sum vanishes unless $m_1 m_2 \equiv n_1 n_2 \pmod p$ in which case it is equal to $p-1$. By [1, Theorem 1], the above congruence has $N^4/p + O(N^2(\log p)^2)$ solutions, which concludes the proof. □

3. Proof of Theorem 1

As in [12] we remark that (2) implies that

$$K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p) = \sum_{n_1=M_1+1}^{M_1+N_1} \cdots \sum_{n_s=M_s+1}^{M_s+N_s} \sum_{n_{s+1}=1}^{p-1} \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} \chi(n_1 \cdots n_{s+1}) \mathbf{e}_p\left(\sum_{\nu=1}^{s+1} a_j n_j\right)$$

$$= \frac{1}{p-1} \sum_{\chi \in \mathcal{X}_p} S_{a_{s+1},\chi}(p) \prod_{\nu=1}^{s} S_{a_\nu,\chi}(M_\nu, N_\nu; p).$$

Thus, using (3), and using the trivial estimate

$$\left|S_{a_\nu,\chi_0}(M_\nu, N_\nu; p)\right| \leqslant N_\nu, \quad \nu = 1, \ldots, s,$$

for the principal character χ_0, we obtain

$$K_s(\mathbf{a}, \mathbf{M}, \mathbf{N}; p) \ll N_1 \cdots N_\nu p^{-1} + p^{-1/2} \sum_{\substack{\chi \in \mathcal{X}_p \\ \chi \neq \chi_0}} \prod_{\nu=1}^{s} \left|S_{a_\nu,\chi}(M_\nu, N_\nu; p)\right|. \tag{4}$$

Now using the Hölder inequality, we deduce

$$\left(\sum_{\substack{\chi \in \mathcal{X}_p \\ \chi \neq \chi_0}} \prod_{\nu=1}^{s} \left|S_{a_\nu,\chi}(M_\nu, N_\nu; p)\right|\right)^s \ll \prod_{\nu=1}^{s} \sum_{\substack{\chi \in \mathcal{X}_p \\ \chi \neq \chi_0}} \left|S_{a_\nu,\chi}(M_\nu, N_\nu; p)\right|^s. \tag{5}$$

It remains to note that for $s \geqslant 2$, by Lemmas 3 and 4 we have

$$\sum_{\substack{\chi \in \mathcal{X}_p \\ \chi \neq \chi_0}} \left|S_{a_\nu,\chi}(M_\nu, N_\nu; p)\right|^s \ll \left(N_\nu^{1-1/r} p^{1/4(r-1)} (\log p)^2\right)^{s-2} \sum_{\chi \in \mathcal{X}_p} \left|S_{a_\nu,\chi}(M_\nu, N_\nu; p)\right|^2$$

$$\ll \left(N_\nu^{1-1/r} p^{1/4(r-1)} (\log p)^2\right)^{s-2} N_\nu p$$

which together with (4) and (5) concludes the proof.

4. Proof of Theorem 2

We argue as in the proof of Theorem 1 except that for $s \geqslant 4$ we use Lemmas 3 and 5 which yield

$$\sum_{\substack{\chi \in \mathcal{X}_p \\ \chi \neq \chi_0}} \left|S_{a_\nu,\chi}(M_\nu, N_\nu; p)\right|^s \ll \left(N_\nu^{1-1/r} p^{1/4(r-1)} (\log p)^2\right)^{s-4} \sum_{\chi \in \mathcal{X}_p} \left|S_{a_\nu,\chi}(M_\nu, N_\nu; p)\right|^4$$

$$\ll \left(N_\nu^{1-1/r} p^{1/4(r-1)} (\log p)^2\right)^{s-4} \left(N_\nu^4 + N_\nu^2 p (\log p)^2\right),$$

which again together with (4) and (5) gives the desired estimate.

5. Further improvements and generalisations

Clearly, if some of $N_1, \ldots, N_s$ are of different order magnitude, then in the proofs of Theorems 1 and 2 one can use Lemma 3 with various values of r for each ν which may lead to stronger bounds. However it seems that the optimal strategy of applying these results heavily depends on various relations between the sizes of $N_1, \ldots, N_s$ and p.

One can extend our results to incomplete multiple Kloosterman sums modulo a composite q. An appropriate version of Lemma 3 is given by D.A. Burgess [4,5] while a variant of Lemma 5 can be derived from a result of J.B. Friedlander and H. Iwaniec [6], but only for special intervals starting at the origin (that is, only for $M_1 = \cdots = M_s = 0$).

We remark that in the cases $s = 1$ and $s = 2$, very short Kloosterman sums have been estimated by A.A. Karatsuba [8,9], M.A. Korolev [10] and more recently by J. Bourgain [2] by using very different arguments. These bounds have found a number of applications to various number theoretic questions, for example, see [7,13]. It would be interesting to find some new applications of incomplete Kloosterman sums for $s \geqslant 3$.

References

[1] A. Ayyad, T. Cochrane, Z. Zheng, The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$ and the mean value of character sums, J. Number Theory 59 (1996) 398–413.
[2] J. Bourgain, More on the sum-product phenomenon in prime fields and its applications, Internat. J. Number Theory 1 (2005) 1–32.
[3] D.A. Burgess, Partial Gaussian sums, Bull. London Math. Soc. 20 (6) (1988) 589–592.
[4] D.A. Burgess, Partial Gaussian sums, II, Bull. London Math. Soc. 21 (2) (1989) 153–158.
[5] D.A. Burgess, Partial Gaussian sums. III, Glasgow Math. J. 34 (2) (1992) 253–261.
[6] J.B. Friedlander, H. Iwaniec, The divisor problem for arithmetic progressions, Acta Arith. 45 (1985) 273–277.
[7] J. Friedlander, H. Iwaniec, The Brun–Titchmarsh theorem, in: Analytic Number Theory, in: London Math. Soc. Lecture Note Ser., vol. 247, 1997, pp. 363–372.
[8] A.A. Karatsuba, Fractional parts of functions of a special form, Izv. Ross. Akad. Nauk Ser. Mat. (Russian Acad. Sci. Izv. Math.) 55 (4) (1995) 61–80 (in Russian).
[9] A.A. Karatsuba, Analogues of Kloosterman sums, Izv. Ross. Akad. Nauk Ser. Mat. (Russian Acad. Sci. Izv. Math.) 55 (5) (1995) 93–102 (in Russian).
[10] M.A. Korolev, Incomplete Kloosterman sums and their applications, Izv. Ross. Akad. Nauk Ser. Mat. (Russian Acad. Sci. Izv. Math.) 64 (6) (2000) 41–64.
[11] R. Lidl, H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge, 1997.
[12] W. Luo, Bounds for incomplete hyper-Kloosterman sums, J. Number Theory 75 (1999) 41–46.
[13] I.E. Shparlinski, On a question of Erdős and Graham, Arch. Math. 78 (2002) 445–448.